UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF INDIANA
FORT WAYNE DIVISION

UNITED STATES OF AMERICA	)	
	)	
v.	)	Cause No. 1:18-CR-83-HAB
	)	
BRADLEY M. COX	)	

OPINION AND ORDER

If anyone needed more motivation to get off social media, consider the instant case. In spring 2018, the FBI was asked to begin an investigation into online extortion of sexual material. They traced the activity to Defendant's employer, where they discovered a virtual private network known to have been involved in the scheme on Defendant's work computer. Agents then questioned Defendant at his home, where he admitted to using multiple Facebook accounts to solicit child pornography and extort sexual material from victims.

Following up on Defendant's confession, the Government sought and obtained a subpoena pursuant to the Stored Communications Act, 18 U.S.C. § 2703(d) (the "SCA"), directed to Facebook. Through the subpoena, the Government obtained registration information, billing records, records of session times and durations, and IP addresses and cookies linked to the accounts used by Defendant (collectively the "Records"). The Government did not obtain the content of any of the accounts.

Defendant now challenges the Government's acquisition of the Records as a warrantless search in violation of the Fourth Amendment. According to Defendant, the Supreme Court's decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), created an exception to the third-party doctrine that protects the Records from being obtained without a warrant. Defendant is not the first person to make this argument. Instead, this same argument has been made by multiple

defendants across the country. To date, no court has accepted the argument, and that streak will not end today.

A. Fourth Amendment

The Fourth Amendment generally requires that the government obtain a warrant based on probable cause before conducting a search. *See Katz v. United States*, 389 U.S. 347, 362 (1967) (Harlan, J., concurring) ("[U]nder the Fourth Amendment, warrants are the general rule."). For an "intrusion into [the] private sphere" to constitute a "search," a defendant must "seek[] to preserve something as private," and "society [must be] prepared to recognize [that privacy expectation] as reasonable." *Carpenter* 138 S. Ct. at 2213 (quoting *Smith v. Maryland*, 442 U.S. 735, 740 (1979)).

Because an individual must seek to preserve something as private before a search can be said to have occurred, information shared with third parties is generally not protected. This is called the third party doctrine. *See Smith*, 442 U.S. at 743-44 (noting that the Supreme Court has "consistently ... held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties") Pursuant to that doctrine, the Supreme Court has separately held that the government need not secure a warrant to obtain recordings of voluntary conversations surreptitiously captured via radio transmitter, *see United States v. White*, 401 U.S. 745, 752-53 (1971), records from banks, *see United States v. Miller*, 425 U.S. 435, 444 (1976), and certain phone call data from pen registers, *see Smith*, 442 U.S. at 745-46, because the information at issue in each instance had been voluntarily disclosed by the defendant to a third party, *see id*. at 743-44.

Defendant does not dispute that he voluntarily disclosed to Facebook (either directly or through associated third-party websites or apps) the information contained in the Records that he now seeks to suppress. He contends, however, that the Supreme Court's decision in *Carpenter*

shows that the third-party doctrine does not apply to the information at issue here and thus that the government needed a warrant to acquire that information.

In *Carpenter*, the defendant challenged on Fourth Amendment grounds the government's warrantless acquisition -- pursuant to the SCA -- of his cell-site location information ("CSLI") from his wireless telecommunications carrier. 138 S.Ct. at 2211-12. The CSLI data acquired in Carpenter depicted the defendant's movements across nearly 13,000 specific location points during a 127-day span. *Id*. at 2212.

The government, in response, invoked the third-party doctrine to justify its warrantless acquisition of the CSLI from the carrier. *Id*. at 2219. The Supreme Court held, however, that the government's acquisition of the CSLI from the carrier constituted a search, for which the government needed a warrant, because Carpenter retained a reasonable expectation of privacy in the CSLI at issue even though he had shared it with his wireless carrier. *Id*. at 2217-20.

Carpenter explained that, given the location information that CSLI conveyed and the fact that a cell phone user transmits it simply by possessing the cell phone, if the government could access the CSLI that it had acquired without a warrant in that case, then the result would be that "[o]nly the few without cell phones could escape" what would amount to "tireless and absolute surveillance." *Id*. at 2218. Carpenter thus declined to extend the third-party doctrine to the CSLI at issue in that case and instead determined that Carpenter did have a reasonable expectation of privacy in the CSLI that he sought to suppress. *Id*. at 2219-20.

Defendant contends that the Records the government acquired from Facebook without a warrant are not materially different from the CSLI that was at issue in *Carpenter*. He notes in this regard that this information enabled the Government to determine his precise location when he logged on to Facebook and associated apps, as well as the date and time of those digital

transmissions. For that reason, he contends, *Carpenter* establishes that the Government needed a warrant to acquire the information from Facebook that he seeks to suppress, because "[a]ll of the relevant factors which make CSLI overly intrusive apply to the location information kept by Facebook, Inc." (ECF No. 133 at 6).

Reasonable minds can debate whether, as a society, we want entities such as Facebook to log the kind of information contained in the Records. But what cannot be debated is that Facebook has this information only by virtue of individuals making an affirmative choice to provide it. Decisions post-*Carpenter* have noted the volitional aspect of IP address collection as a key point of distinction from CSLI. *See, e.g.*, *United States v. Hood*, 920 F.3d 97, 92 (1st Cir. 2019) ("an internet user generates the IP address data that the government acquired from Kik in this case only by making the affirmative decision to access a website or application. By contrast, as the Supreme Court noted in *Carpenter*, every time a cell phone receives a call, text message, or email, the cell phone pings CSLI to the nearest cell site tower without the cell phone user lifting a finger."); *see also United States v. Caira*, 833 F.3d 803, 808 (7th Cir. 2016) ("the government only received record of the I.P. addresses Caira used to log in to his Hotmail account. . . . On days when he did not log in, the government had no idea where he was."). Defendant's own filings demonstrate this point: Defendant identifies several instances where Facebook logs a user's IP address, including "changing account information to sending attachments in private messages to uploading photos to the profile," amongst other "events [that] occur during the normal course of using Facebook as intended." (ECF No. 133 at 5). All these events require affirmative action by the user. Indeed, Defendant has not identified a single instance where Facebook creates an IP log without user action. Defendant is correct that the Records contain potentially personal information about his

life, but they contain no more than he chose to provide.[1] This fact, in and of itself, takes the Records outside of the scope of *Carpenter*. *See, e.g., United States v. Kidd*, 349 F.Supp.3d 357, 366 (S.D.N.Y. 2019) (holding that defendant needed to establish that his cell phone: "(1) passively generates IP address information for Pinger to collect in a way similar to CSLI; or (2) consistently conveys granular location information.").

Defendant also overstates the precision of the information gathered from the Records. Defendant's characterization of the Records as providing his "exact location" is, as the Seventh Circuit has recognized, an "unhelpful exaggeration." *Id*. at 808. Rather, "the IP address data that the government acquired from [Facebook] does not itself convey any location information. The IP address data is merely a string of numbers associated with a device that had, at one time, accessed a wireless network." *Hood*, 920 F.3d at 92. As the Government correctly notes, that string of numbers means nothing without additional investigation, including but not limited to gathering specific user and location information from an internet service provider. (ECF No. 137 at 11, n. 5). While this fact is not necessarily determinative, *see Kidd*, 394 F.Supp.3d at 365–66, it does weigh against finding that the Records act as a tracking device.

The legal issues aside, Defendant's motion fails for a more fundamental reason. All the information contained in Defendant's filings regarding the Records, their contents, and the ability of the Government to use the Records for tracking purposes comes solely from Defendant. Throughout his filings, Defendant makes hyperbolic statements like the Records reveal his "exact location" (ECF No. 133 at 5); that they create "a detailed chronicle of [his] physical presence" (*Id*.

[1] Defendant argues that the fact that "devices will remain logged in to Facebook" undermines the argument that information is knowingly submitted by the user. (ECF No. 133 at 6). The Court cannot agree (since the IP logs appear to only be created through user activity), but even if it did the argument ignores the fact that leaving Facebook logged on is itself a decision. There is nothing that stops a user from logging out of Facebook or an associated app when they are finished using it. That they choose not to out of convenience, laziness, or any other motivation does not change the volitional nature of the information transfer.

at 6); that they provide "an intimate window into a person's life" (*Id.*); that the Records are "distinctly more comprehensive than the typical IP logs" (ECF No. 138 at 5); and that the cookie data is like "the names and account numbers of every person who used a particular ATM" (*Id.* at 9). However, Defendant has no expert to opine on the extent of the Records, nor does he provide any other admissible evidence regarding their nature or potential use. The Court has not even been provided with the Records or any part thereof. Since Defendant has the burden of establishing his reasonable expectation of privacy, *see Kidd*, 394 F.Supp.3d 357 at 366, this lack of evidence is fatal to the motion.

Moreover, Defendant consistently undermines any credibility his pronouncements might have. Defendant compares the Records to CSLI data throughout his filings but admits in his reply that he has "never seen CSLI data." (ECF No. 138). Defendant argues that Facebook is ubiquitous but admits that he had done no research on the breadth of Facebook usage and further admits that his representations in this regard are a "guess." (ECF No. 133 at 2–3). Defendant portrays the information gathered by Facebook as being significantly more intrusive than other companies, but ultimately is forced to admit simply that *he* knows of no other company that records and reports such data. (ECF No. 138 at 8). The Court would not be inclined to take a party's word for any determinative proposition and is much less inclined to do so when the party has made clear that his word is based on little more than guess and speculation.

And even if Defendant's hyperbole was accurate generally, he makes no attempt to demonstrate that it is accurate with respect to this case. Take, for instance, Defendant's assertion that the cookie data can reveal the online activity of third parties. (*Id.* at 9). Did that happen in this case? The Court has reviewed the filings of both Defendant and the Government and finds no evidence that it did. Perhaps more to the point, Defendant has not so much as designated a single

instance where the Government was able to determine his location from the Records. This Court's Fourth Amendment analysis is not driven by what might be possible or what could have happened. Instead, this Court must undertake a "fact-specific inquiry." *United States v. Burnside*, 588 F.3d 511, 517 (7th Cir. 2009). Defendant has told the Court nothing about the evidence adduced from the Records, giving the Court no ability to meaningfully analyze whether that evidence should be stricken.

The evolution of technology may one day change the analysis on this issue. *Carpenter* was not decided until 2018, nearly two decades after cell phones had achieved widespread adoption. We may one day wake up and find that Facebook or some other social network has become as indispensable as the cell phone and determine, as a society, that the information collected is deserving of constitutional protection. But that day is not today, and this case is not that case. On the basis of the record before the Court, the Records "fall[] comfortably within the scope of the third-party doctrine" which continues, even after *Carpenter*, to apply to "business records that might incidentally reveal location information." *United States v. Contreras*, 905 F.3d 853, 857 (5th Cir. 2018). As such, Defendant had no reasonable expectation of privacy in the Records, and no Fourth Amendment violation occurred.

B. Good Faith

Even if the Court were to rule differently on the Fourth Amendment issue, it would still be compelled to deny Defendant's motion. The exclusion of evidence seized in violation of the Fourth Amendment is "a judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect, rather than a personal constitutional right of the party aggrieved." *United States v. Leon*, 468 U.S. 897, 906 (1984) (quoting *United States v. Calandra*, 414 U.S. 338, 348 (1974).

> The deterrent purpose of the exclusionary rule necessarily assumes that the police have engaged in willful, or at the very least negligent, conduct which has deprived the defendant of some right. By refusing to admit evidence gained as a result of such conduct, the courts hope to instill in those particular investigating officers, or in their future counterparts, a greater degree of care toward the rights of an accused. Where the official action was pursued in complete good faith, however, the deterrence rationale loses much of its force.

Michigan v. Tucker, 417 U.S. 433, 447 (1974). Accordingly, where the illegal seizure is the result of "objectively reasonable law enforcement activity," the exclusionary rule does not apply. *Leon*, 468 U.S. at 919. Objectively reasonable law enforcement activity has been found both where officers rely on a search warrant, *Leon*, 468 U.S. at 920–21, and where they rely on a statute that is later declared unconstitutional, *Illinois v. Krull*, 480 U.S. 340, 352 (1987).

That *Carpenter* did not invalidate the SCA in its entirety does not meaningfully distinguish this case from *Krull*. What matters is whether the Government could reasonably rely on the SCA at the time the subpoena was issued to Facebook. Defendant argues that it could not, pointing to language at the end of the Sixth Circuit's ruling on remand in *Carpenter*. There, that court held, "[m]oving forward, traditional Fourth Amendment principles will replace reflexive or mechanical use of § 2703(d). The government must either get a warrant or rely on a recognized exception to the warrant requirement." *United States v. Carpenter*, 926 F.3d 313, 318 (6th Cir. 2019).

Read out of context, this passage seems to suggest that all requests under the SCA require either a warrant or a recognized exception. This would support Defendant's arguments. But read in context, it is clear that the Sixth Circuit limited its holding to CSLI. This is true not only because CSLI was the sole issue before the court, but also because CSLI is explicitly referenced in the sentence immediately preceding Defendant's chosen excerpt. *Carpenter*, supra ("*Carpenter II* confirmed that the SCA does not immunize a government officer's collection of CSLI from the

safeguards of the Fourth Amendment."). The Court finds nothing in the Sixth Circuit's holding that would have put the Government on notice that a warrant was required to obtain the Records.

The insurmountable obstacle for Defendant is the unanimity of case law that holds contrary to his suppression argument. "Evidence obtained during a search conducted in reasonable reliance on binding precedent is not subject to the exclusionary rule." *Davis v. United States*, 564 U.S. 229, 241 (2011). As the Government points out, every federal appellate and trial court, including the Seventh Circuit, that has ruled on the question of whether individuals have a reasonable expectation of privacy in IP logs has answered in the negative. (*See* ECF No. 137 at 12–13) (collecting cases). Absent any authority to the contrary, the Government was entitled to rely on those precedents, both binding and persuasive. Therefore, even if the Government conducted a search in violation of the Fourth Amendment when it obtained the Records, the Court concludes that it acted in good faith.

C. Conclusion

For the foregoing reasons, Defendant's Motion to Suppress (ECF No. 133) is DENIED.

SO ORDERED on June 3, 2020.

s/ Holly A. Brady
JUDGE HOLLY A. BRADY
UNITED STATES DISTRICT COURT